Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application. Please amend the claims as follows:

Listing of Claims:

1. (Currently Amended) A method for negotiating a set of security parameters usable by an initiator and a responder to create a secure path over a network for exchanging information, the method including a plurality of modes, comprising:

conducting an internet key management and exchange protocol (IKE) main mode negotiation for establishing the secure path and selecting the set of security parameters including a security protocol;

conducting an internet key management and exchange protocol (IKE) quick mode negotiation for deriving a set of keys usable with the security protocol;

wherein a ~~at least one~~ message is exchanged between the responder and the initiator before the completion of the IKE main mode negotiation, [[that]] the message comprising [[comprises]] at least part of the IKE quick mode negotiation, and the message including both a main mode pseudo random number ~~is sent during the IKE main mode negotiation~~ and a separate quick mode pseudo random number ~~is exchanged between the responder and the initiator before completion of the IKE main mode negotiation~~; and

wherein a protocol security process establishes inbound and outbound protocol security associations.

2. (Original) The method of claim 1, further comprising:

conducting a first user mode for authenticating a first user associated with the initiator or responder.

3. (Previously Presented) The method of claim 2, wherein the initiator and the responder exchange authentication data that is calculated by application of a hash function incorporating a secret key on data exchanged during the IKE main mode negotiation.

4. (Original) The method of claim 2, further comprising:

conducting a second user mode for authenticating a second user associated with the initiator or the responder.

5. (Previously Presented) The method of claim 1, wherein the IKE main mode comprises:

sending, from the initiator to the responder, a set of proposed security parameters and authentication data;

selecting, by the responder, the set of security parameters from the set of proposed security parameters;

sending the set of security parameters from the responder to the initiator.

6. (Previously Presented) The method of claim 1, wherein the initiator identifies a public key of the responder prior to the IKE main mode negotiation and wherein at least a portion a first message sent from the initiator to the responder is encrypted using the public key.

7. (Previously Presented) The method of claim 1, wherein the IKE main mode negotiation comprises:

sending a group advertisement from the initiator to the responder;

comparing the group advertisement to a set of authorized groups; and

sending a response from the responder to the initiator.

8. (Previously Presented) The method of claim 1, further comprising:

exchanging Diffie Hellman key data between the initiator and the responder during IKE main mode for deriving keys for use with an encryption algorithm.

9. (Original) The method of claim 1, further comprising:

exchanging a pair of notify payloads between the initiator and the responder; wherein the pair of notify payloads are used by the protocol security process for establishing the protocol security associations.

10 - 17. (Canceled)

18. (Currently Amended) A computer storage medium encoding computer-readable instructions for negotiating a set of security parameters usable by an initiator and a responder to create a secure path over a network for exchanging information, the method including a plurality of modes, comprising:

conducting an internet key management and exchange protocol (IKE) main mode negotiation for establishing the secure path and selecting the set of security parameters including a security protocol;

conducting an internet key management and exchange protocol (IKE) quick mode negotiation for deriving a set of keys usable with the security protocol;

wherein a ~~at least one~~ message is exchanged between the responder and the initiator before completion of the IKE main mode negotiation, [[that]] the message comprising [[comprises]] at least part of the IKE quick mode negotiation, and the message including both a main mode pseudo random number ~~is sent during the IKE main mode negotiation~~ and a separate quick mode pseudo random number ~~is exchanged between the responder and the initiator before completion of the IKE main mode negotiation~~; and

wherein a protocol security process establishes protocol security associations.

19. (Previously Presented) The computer storage medium of claim 18, further comprising:

conducting a user mode for authenticating one or more users associated with the initiator or the responder.

20. (Previously Presented) The computer storage medium of claim 19, wherein the initiator and the responder exchange authentication data that is calculated by application of a hash function incorporating a secret key on data exchanged during the IKE main mode negotiation.

21. (Previously Presented) The computer storage medium of claim 18, wherein the initiator identifies a public key of the responder prior to the IKE main mode negotiation and wherein at least a portion a first message sent from the initiator to the responder is encrypted using the public key.

22. (Previously Presented) The computer storage medium of claim 18, wherein the IKE main mode comprises:

sending a group advertisement from the initiator to the responder;

comparing the group advertisement to a set of authorized groups; and

sending a response from the responder to the initiator.

23 - 25. (Canceled)

26. (Currently Amended) A method for negotiating a set of security parameters usable by an initiator and a responder to create a secure path over a network for exchanging information, the method comprising:

sending, from the initiator, a first message, wherein the first message comprises part of an internet key management and exchange protocol (IKE) main mode negotiation and the IKE main mode negotiation comprises establishing the secure path and selecting a set of security parameters including a security protocol;

receiving, at the initiator, a second message, wherein the second message comprises at least part of the IKE main mode negotiation and at least part of an internet key management and exchange protocol (IKE) quick mode negotiation and the IKE quick mode negotiation comprises deriving a set of keys usable with the security protocol and wherein the second message includes both a main mode pseudo random number and a separate quick mode pseudo random number;

sending, from the initiator, a third message after receiving the second message, wherein the third message comprises at least part of the IKE main mode negotiation; and

wherein a protocol security process establishes inbound and outbound protocol security associations at the initiator.

27. (Currently Amended) A method for negotiating a set of security parameters usable by an initiator and a responder to create a secure path over a network for exchanging information, the method comprising:

receiving, at the responder, a first message, wherein the first message comprises at least part of an internet key management and exchange protocol (IKE) main mode negotiation and the IKE main mode negotiation comprises establishing the secure path and selecting a set of security parameters including a security protocol;

sending, from the responder, a second message, wherein the second message comprises at least part of the IKE main mode negotiation and at least part of an internet key management and exchange protocol (IKE) quick mode negotiation and wherein the IKE quick mode negotiation comprises deriving a set of keys usable with the security protocol and wherein the second message includes both a main mode pseudo random number and a separate quick mode pseudo random number; and

wherein a protocol security process establishes inbound and outbound protocol security associations.